# Ciberataques: La concienciación ya no es algo opcional

Cyber Guru

# Introducción

El factor humano es ahora el elemento más crucial de la ciberseguridad y los ciberdelincuentes lo utilizan para introducirse en las organizaciones con estrategias ofensivas cada vez más sofisticadas. De hecho, son precisamente los usuarios los que abren sin saberlo la puerta a los atacantes al no adecuar sus comportamientos a la complejidad del reto.

Al analizar los diversos informes sobre el estado de la ciberseguridad, el cuadro que emerge es que el crecimiento de los ataques cibernéticos parece imparable y que, entre las diversas técnicas de ataque utilizadas, las que se caracterizan por un mayor crecimiento se basan principalmente en el factor humano.

Los registros están llenos de ciberataques satisfactorios. Ataques que afectaron a empresas de todos los sectores y de todos los tamaños. Marcas prestigiosas y otras menos conocidas han visto sus actividades productivas bloqueadas y su reputación comprometida. Se trata de una verdadera guerra cibernética que ve a los atacantes en una posición de indudable ventaja, sobre todo porque la primera línea de defensa está formada por usuarios poco formados que, en la mayor parte de los casos, ni siquiera se dan cuenta de que les están atacando.

Por lo tanto, lanzar programas de concienciación sobre ciberseguridad eficaces e innovadores, capaces de afectar al comportamiento humano y convertir a los usuarios en la primera línea de defensa de las organizaciones, ya no es algo opcional.

El objetivo de la plataforma de concienciación sobre ciberseguridad de Cyber Guru es precisamente aumentar la resistencia a los ciberataques a través de vías de aprendizaje permanente capaces de desarrollar en las personas la capacidad de actuar con un comportamiento seguro determinado por una mayor concienciación.
Una plataforma constantemente implementada que utiliza las tecnologías, los procesos de producción y las metodologías pedagógicas más avanzadas para garantizar la máxima participación de los usuarios y la protección contra los riesgos cibernéticos.

**Mar Sánchez**
Sales Country Manager España

# El escenario

Las tendencias de los ataques cibernéticos de los últimos años muestran una curva en constante crecimiento. Una de las principales causas es, sin duda, el aumento del uso de las tecnologías digitales, considerado el motor del crecimiento económico real. No obstante, este aumento no ha ido acompañado de un nivel adecuado de alfabetización digital entre los usuarios. Los efectos de la pandemia aceleran esta tendencia con el uso masivo del teletrabajo y el mayor uso de aplicaciones y servicios digitales.

Desgraciadamente, a pesar de los considerables esfuerzos realizados por las empresas en materia de ciberseguridad, lo que se constata es que el eslabón más débil de la cadena de defensa de cualquier empresa sigue siendo el factor humano y, en particular, los usuarios digitales. De hecho, en la actualidad se ha comprobado que más del 90% de los ciberataques tienen su origen en un error humano, en un comportamiento inadecuado.

**El 90% de los ciberataques comienzan con un clic en un correo electrónico malicioso**

Barclays Bank

**El 95% de los ciberataques se deben a un error humano**

IBM Cyber Security Intelligence Index Report

# La fuerza de una cadena depende de su eslabón más débil

La resistencia global de una empresa a los ciberataques depende, por tanto, de la resistencia del factor humano, el verdadero eslabón débil de la cadena en la actualidad.

El desarrollo de la sociedad digital, con sus riesgos, obliga a todas las organizaciones a invertir de manera sustancial en el factor humano, especialmente en el nivel de concienciación de las personas.

Una inversión que ha pasado a ser necesaria para cerrar la brecha cultural que los efectos de la pandemia y la rápida transformación digital han agudizado.

**En 2021, las filtraciones de datos costarán a las empresas 45 000 millones de dólares**

Panda Security

**El número de ataques de «ransomware» aumentó un 13% entre 2020 y 2021**

Verizon Data Breach Investigations Report

**El coste mundial de la ciberdelincuencia alcanzará los 10,5 billones de dólares en 2025**

Cybersecurity Ventures

# La metodología

Por lo tanto, lanzar programas de concienciación sobre ciberseguridad eficaces e innovadores, capaces de transformar el comportamiento humano y convertir a los usuarios en la primera línea de defensa de las organizaciones, ya no es algo opcional.

La plataforma Cyber Guru está diseñada para maximizar los procesos de aprendizaje mediante el desarrollo de 3 características defensivas del individuo: **conocimiento**, **percepción del peligro y preparación**.

Esto requiere programas de formación avanzados, basados en metodologías innovadoras de formación permanente y compromiso, que minimicen el impacto en la formación del personal y las funciones de gestión de la ciberseguridad. Solo así será posible seguir la evolución constante de estrategias de ataque cada vez más sofisticadas.

## 3 ITINERARIOS FORMATIVOS

### Cognitivo

Los conocimientos se gestionan mediante un proceso de formación cognitiva basado en un enfoque principalmente didáctico

### Inductivo

La percepción del peligro se estimula mediante un entrenamiento inductivo que tiende a actuar sobre el componente más emocional de nuestro cerebro

### Experiencial

La formación del estado de alerta es esencial para actuar rápidamente y adoptar el comportamiento adecuado cuando surge un peligro

# Una plataforma integral de concienciación sobre ciberseguridad

La plataforma está diseñada para transformar el comportamiento de la plantilla de cualquier empresa pública o privada, sea cual sea su tamaño o categoría de producto, mediante:

**3 ITINERARIOS FORMATIVOS REALMENTE SINÉRGICOS**

## Cyber Guru Awareness

Un programa educativo cognitivo impartido sobre una base de aprendizaje electrónico que garantiza el desarrollo gradual de la concienciación mediante el conocimiento de las amenazas de la red y las pautas de comportamiento que deben adoptarse para prevenir los ataques.

## Cyber Guru Channel

Un programa de formación inductiva que genera aprendizaje a través del poder de la narración y la producción de vídeo. Siguiendo un patrón narrativo típico de las series de televisión, el alumno aprende identificándose con las situaciones narradas en los diferentes episodios.

## Cyber Guru Phishing

Un programa de formación experiencial que capacita a las personas para resistir los distintos tipos de ataques de «phishing». El programa, automático y adaptativo, permite personalizar el entrenamiento en función de la experiencia individual y del nivel de resistencia individual a los ataques.

# Cyber Guru Awareness

Cyber Guru Awareness se ha diseñado para que toda la empresa participe en un itinerario de aprendizaje educativo y estimulante que se caracteriza por su enfoque de «desarrollo constante y gradual» («Smart-School»). El itinerario consta de módulos de formación autocoherentes, cada uno dedicado a un tema específico, con activación mensual durante un periodo de 12, 24 o 36 meses. Cada módulo se compone a su vez de 3 lecciones breves en vídeo de 5 minutos cada una. Las principales características son el aprendizaje cognitivo eficaz, la máxima implicación del alumno y la supervisión de impacto cero.

- **Módulos formativos autoconsistentes de activación mensual**
- **Compromiso mínimo semanal, compatible con cualquier función**
- **Microlecciones en vídeo en formato multimedia**
- **Uso de actores profesionales con funciones de «coach»**
- **Lenguaje altamente divulgativo**
- **Enfoque interactivo con alternancia continua entre microlecciones y pruebas**
- **Test de evaluación de respuesta múltiple**
- **Metodología de ludificación, con organización en equipos**
- **Plataforma multilingüe**
- **Contenidos adicionales y constantemente actualizados**

# Cyber Guru Channel

La metodología inductiva utilizada se basa en la inmersión del usuario en una situación real y en un proceso de autoidentificación con la ciberamenaza, que adopta una forma concreta. El usuario toma conciencia a través de una narración, que actúa, primero, sobre la percepción del peligro y, posteriormente, sobre el elemento memorista en vez de a través de una noción, lo que va más allá del peligroso «a mí no me puede pasar». Las tres principales características son el aprendizaje inductivo eficaz, la máxima implicación del alumno y la supervisión de impacto cero.

- **Formación continua**
- **Producciones de vídeo avanzadas**
- **Múltiples formatos de vídeo con diferentes narrativas**
- **Episodios cortos**
- **Alto ritmo narrativo**
- **Autoidentificación en situaciones realistas**
- **Enfoque al estilo de Netflix**
- **Documentación detallada de cada episodio**
- **Informes avanzados sobre el nivel de aprovechamiento**
- **Funciones de atención al estudiante para motivar la participación**

# Cyber Guru Phishing

Cyber Guru Phishing se ha diseñado para que la plantilla entrene cómo resistir ataques de «phishing», a través de campañas de ataques simulados, que se personalizan según el perfil de comportamiento de cada usuario, gracias a un proceso automático y adaptativo, guiado por el uso de técnicas de inteligencia artificial. El alumno aumenta su resistencia a los ataques mediante la experiencia, tanto la experiencia negativa del error como la experiencia positiva de reconocer el ataque. Las tres características principales son la formación experiencial eficaz, el «coaching» personalizado y la supervisión de impacto cero.

- **Formación experiencial eficaz y continua**
- **Formación personalizada mediante un proceso adaptativo**
- **Niveles de dificultad y simulaciones personalizadas**
- **Campañas de ataque automatizadas**
- **Error -> Formación instantánea**
- **Procedimiento de notificación**
- **Plantillas precargadas**
- **Informes analíticos y de gestión a través de un cuadro de mando avanzado**
- **Grupos de riesgo**
- **Políticas de subsanación**

# Cyber Guru

## Security Awareness Training That Works!

Síguenos en LinkedIn | Youtube

Más información en Cyber Guru
cyberguru.it/es/

Conviértete e nuestro socio
cyberguru.it/es/partner/

¿Quieres ver una demostración en directo de nuestras soluciones?

Reserva una cita de 30 minutos con un especialista en formación en concienciación

RESERVAR AHORA